What is claimed is:

1. A method for enabling a primary conditional access provider (CAP) and at least one secondary CAP to provide conditional access (CA) data in respective different formats to control access to at least one data service, comprising the steps of:

(a) providing, at the primary CAP, first CA data in a first format for encrypting the at least one data service during a plurality of successive crypto-periods, and time data for identifying the successive crypto-periods;

(b) providing the first CA data and the time data from the primary CAP to the at least one secondary CAP;

wherein the at least one secondary CAP is responsive to the first CA data and time data for providing second CA data in a different, second format for the successive crypto-periods; and

(c) providing a data stream comprising the at least one encrypted data service and first and second CA data to user terminals, including at least a first user terminal that is compatible with the first CA data, and a second user terminal that is compatible with the second CA data.

2. The method of claim 1, wherein;

the time data indicates respective start times of the crypto-periods.

3. The method of claim 2, wherein:

the time data designates absolute times of the crypto-periods.

4. The method of claim 2, wherein:

the time data designates relative times of the crypto-periods in relation to a reference time of the at least one data service.

5. The method of claim 1, wherein:

the first CA data for each crypto-period is provided to the at least one secondary CAP with a lead time of at least one crypto-period.

6. The method of claim 5, wherein:

the lead time is responsive to a required processing time of the at least one secondary CAP.

7. The method of claim 5, wherein:

the first CA data and time data are provided to the at least one secondary CAP in successive packets, each packet comprising first CA data and time data for a plurality of crypto-periods.

8. The method of claim 7, wherein:

the plurality of crypto-periods comprise a current crypto-period and future crypto-periods.

9. The method of claim 1, wherein:

the first CA data comprises a control word for each of the crypto-periods.

10. The method of claim 1, wherein:

the first CA data and time data are streamed in real-time from the primary CAP to the at least one secondary CAP without being requested therefrom.

11. The method of claim 10, wherein:

the at least one secondary CAP provides its second CA data essentially in real-time after receipt of the first CA data and time data thereat.

12. The method of claim 1, comprising the further steps of:

synchronizing the first CA data and the second CA data with the at least one encrypted data service; and

storing the first and second synchronized CA data and the at least one encrypted data service for subsequent retrieval to provide said data stream.

13. The method of claim 12, comprising the further step of:

retrieving the first and second synchronized CA data and the at least one encrypted data service to provide said data stream in response to a user request.

14. The method of claim 13, wherein:

the user request is provided as part of a video-on-demand service.

15. The method of claim 1, wherein:

the primary CAP provides a program identifier to the at least one secondary CAP to inform the at least one secondary CAP that the first CA data and the time data are associated with the at least one data service.

16. The method of claim 1, wherein:

the first CA data and time data are provided from the primary CAP to the at least one secondary CAP via a CA data delivery network.

17. The method of claim 1, wherein:

the first and second CA data are provided to a message insertion subsystem out-of-band from the encrypted data service to form said data stream.

18. The method of claim 1, wherein:

the first and second CA data are provided to a message insertion subsystem in-band with the encrypted data service to form said data stream.

19. The method of claim 1, wherein:

the first CA data and the time data are provided from the primary CAP to a plurality of secondary CAPs, each of which is responsive to the first CA data and time data for providing CA data in different, respective formats for the successive crypto-periods;

the data stream comprises the CA data in the different, respective formats; and

the user terminals include respective user terminals that are compatible with the different, respective formats.

20. The method of claim 1, wherein:

the first CA data, time data, and encrypted data service are provided in a first data stream from the primary CAP to the at least one secondary CAP for

insertion of the second CA data, and a corresponding second data stream is returned to the primary CAP for formation of said data stream that is provided to the user terminals.

21. The method of claim 20, comprising the further steps of:

retaining a copy of the first data stream at the primary CAP;

filtering, at the primary CAP, the second data stream that is returned from the at least one secondary CAP to recover the second CA data; and

combining the recovered second CA data with the retained copy of the first data stream to form said data stream that is provided to the user terminals.

22. The method of claim 20, comprising the further steps of:

retaining a copy of the first data stream at the primary CAP; and

comparing, at the primary CAP, the second data stream to the retained copy of the first data stream to determine a deviation therebetween.

23. The method of claim 22, comprising the further step of:

if the deviation is detected, using the retained copy of the first data stream, which does not contain the second CA data, to form said data stream that is provided to the user terminals.

24. The method of claim 20, wherein:

the second data stream is formed by overwriting the first CA data with corresponding second CA data in corresponding packets of the first data stream.

25. The method of claim 1, wherein:

the first CA data comprises entitlement control messages.

26. The method of claim 1, wherein:

the primary CAP first and at least one secondary CAPs are provided at a headend.

27. The method of claim 1, wherein the first CA data is provided from the primary CAP to the at least one secondary CAP in an encrypted form, comprising the further step of:

providing data to the at least one secondary CAP for decrypting the encrypted first CA data.

28. An apparatus for enabling a primary conditional access provider (CAP) and at least one secondary CAP to provide conditional access (CA) data in respective different formats to control access to at least one data service, comprising:

a primary CAP for providing first CA data in a first format for encrypting the at least one data service during a plurality of successive crypto-periods, and time data for identifying the successive crypto-periods;

means for communicating the first CA data and the time data from the primary CAP to the at least one secondary CAP;

wherein the at least one secondary CAP is responsive to the first CA data and time data for providing second CA data in a different, second format for the successive crypto-periods; and

means for providing a data stream comprising the at least one encrypted data service and first and second CA data to user terminals, including at least a first user terminal that is compatible with the first CA data, and a second user terminal that is compatible with the second CA data.